This is a published notice on the Find a Tender service: https://www.find-tender.service.gov.uk/Notice/002694-2025

Not applicable

Communication Exploitation Data Tool (CEDT)

Mayor's Office of Policing and Crime

F14: Notice for changes or additional information

Notice identifier: 2025/S 000-002694
Procurement identifier (OCID): ocds-h6vhtk-04d526
Published 27 January 2025, 12:35pm

Section I: Contracting authority/entity

I.1) Name and addresses

Mayor's Office of Policing and Crime

New Scotland Yard

LONDON

SW1A2JL

Email

NCTPHQMailbox-.Commercial@met.police.uk

Country

United Kingdom

Region code

UK - United Kingdom

Justification for not providing organisation identifier

Not on any register

Internet address(es)

Main address

www.met.police.uk

Buyer's address

https://supplier.coupahost.com/sessions/new

Section II: Object

II.1) Scope of the procurement

II.1.1) Title

Communication Exploitation Data Tool (CEDT)

II.1.2) Main CPV code

- 48900000 - Miscellaneous software package and computer systems

II.1.3) Type of contract

Supplies

II.1.4) Short description

The Authority requires a national software capability service tool which:

1. Processes, cleanse, and analyses, large amounts of communications data in varying formats for investigation purposes.

2. Enables intelligence analysts to analysis, generate timelines, reports, i2 charts, and rich maps to visualise key insights and patterns from the communications data.

3. Operates as a connected solution, accessible via force computers and integrate with existing secure data transfer processes, while ensuring compliance with the Authority's security protocols and data handling legislation

Some key critical compliance requirements are set out in the Additional Information section below.

Section VI. Complementary information

VI.6) Original notice reference

Notice number: 2025/S 000-002077

Section VII. Changes

VII.1.2) Text to be corrected in the original notice

Section number

II.2.4

Place of text to be modified

Description of the procurement

Instead of

Text

II.2.4) Description of the procurement

Must requirements:

The solution must cleanse raw communications data, including radio frequency data, and transform it into standardised, usable format suitable for intelligence analysis.

The solution must support importing and process data from multiple file formats, including but not limited to; CSV, ANPR data, Drone Data, Zipcar records, Uber Ride Data, Uber Eats delivery Data.

The supplier's solution should be zero deployment and accessible via a browser to be suitable.

The solution shall be accessible via a standard internet browser - i.e. Microsoft Edge and Google Chrome.

The supplier's solution must ensure that all data is: Encryption in-transit, using secure protocols (e.g., Transport Layer Security (TLS) TLS1.2, higher, comparable). Encrypted at rest, utilising industry-standard encryption algorithms (e.g., AES-256).

The supplier's solution must implement robust access control mechanisms, including Role-Based Access Control (RBAC) to restrict access based on user roles and responsibilities.

Supplier shall provide training and training material to the Authority for the tool.

Supplier shall be fully responsible for the support and maintenance of their servers.

Read

Text

II.2.4) Description of the procurement

Must requirements:

The solution must cleanse raw communications data, including radio frequency data, and transform it into standardised, usable format suitable for intelligence analysis.

The solution must support importing and process data from multiple file formats, including but not limited to; CSV, ANPR data, Drone Data, Zipcar records, Uber Ride Data, Uber Eats delivery Data.

The supplier's solution should be zero deployment and accessible via a browser to be suitable.

The solution shall be accessible via a standard internet browser - i.e. Microsoft Edge and Google Chrome.

The supplier's solution must ensure that all data is: Encryption in-transit, using secure protocols (e.g., Transport Layer Security (TLS) TLS1.2, higher, comparable). Encrypted at rest, utilising industry-standard encryption algorithms (e.g., AES-256).

The supplier's solution must implement robust access control mechanisms, including Role-Based Access Control (RBAC) to restrict access based on user roles and responsibilities.

Supplier shall provide training and training material to the Authority for the tool.

Supplier shall be fully responsible for the support and maintenance of their servers.

This notice intends to inform the marketplace of a potential upcoming tender opportunity. The procurement documentation will be made available following the publication of the Contract Notice, which will mark the start of the procurement process. This is anticipated to be late February 2025.

Procurement documentation will be accessible via the URL link referenced in I.3 section.